

Math 125 Class notes

Spring 2026

To accompany
Discrete Mathematics with Applications
by Epp

Peter Westerbaan

Last updated: February 16, 2026

Table Of Contents

| | |
|---|----|
| 1.1: Variables | 1 |
| 1.2: The Language of Sets | 6 |
| 1.3: The Language of Relations and Functions | 14 |
| 2.1: Logical Form and Logical Equivalence | 19 |
| 2.2: Conditional Statements | 28 |
| 2.5: Application: Number Systems and Circuits for Addition | 35 |
| 3.1: Predicates and Quantified Statements I | 44 |
| 3.2: Predicates and Quantified Statements II | 49 |
| 6.1: Set Theory: Definitions and the Element Method of Proof | 54 |
| 6.4: Boolean Algebras, Russell's Paradox, and the Halting Problem | 63 |

1.1: Variables

Definition.

A **variable** is a placeholder for something which may or may not be unknown.

Example. Is there a number with the following property: doubling it and adding 3 gives the same result as squaring it?

- Is there a number x with the property that $2x + 3 = x^2$?
- Is there a number \square with the property that $2 \cdot \square + 3 = \square^2$?

Example. No matter what number might be chosen, if it is greater than 2, then its square is greater than 4.

- No matter what number n might be chosen, if n is greater than 2,
then n^2 is greater than 4.

Example. Use variables to rewrite the following sentences:

Are there numbers with the property that the sum of their squares equals the square of their sum?

Given any real number, its square is nonnegative.

Definition.

- A **universal statement** says that a certain property is true for all elements in a set.
- A **conditional statement** says that if one thing is true, then some other thing also has to be true.
- Given a property that may or may not be true, an **existential statement** says that there is at least one thing for which the property is true.

Definition.

A **universal conditional statement** is both universal and conditional:

For every animal a , if a is a dog, then a is a mammal.

Conditional statements can be rewritten in ways that make them appear more to be purely universal or purely conditional:

If a is a dog, then a is a mammal.

All dogs are mammals

Example. Rewrite the following universal condition statement:

For every real number x , if x is nonzero then x^2 is positive.

If a real number is nonzero, then its square _____.

For every nonzero real number x , _____.

If x _____, then _____.

The square of any nonzero real number is _____.

All nonzero real numbers have _____.

Definition.

A **universal existence statement** is a statement that is universal because its first part says that a certain property is true for all objects of a given type, and it is existential because its second part asserts the existence of something:

Every real number has an additive inverse.

In the above example, note that the particular additive inverse depends on the given real number:

For every real number r , there is an additive inverse for r .

Example. Rewrite the following universal existence statement:

Every pot has a lid

All pots _____.

For ever pot P , there is _____.

For every pot P , there is a lid L such that _____.

Definition.

An **existential universal statement** is a statement that is existential because its first part asserts that a certain object exists and is universal because its second part says that the object satisfies a certain property for all things of a certain kind:

There is a positive integer that is less than or equal to every positive integer.

The number one satisfies the above statement, which can also be rewritten:

There is a positive integer m that is less than or equal to every positive integer.

Example. Rewrite the following existence universal statement:

There is a person in my class who is at least as old as every person in my class.

Some _____ is at least as old as _____.

There is a person p in my class such that p is _____.

There is a person p in my class with the property that for every person q in my class, p is _____.

1.2: The Language of Sets

Definition.

- A **set** is a collection of objects.
- If S is a set, then we use
 - $x \in S$ to denote that the element x is in the set S .
 - $x \notin S$ to denote that the element x is *not* in the set S .
- The **set-roster notation** is used to denote all elements in a set between braces:

$$S = \{1, 2, \dots, 100\}$$

Here, we see that $67 \in S$, but $1337 \notin S$.

- The **axiom of extension** says that a set is completely determined by what its elements are – not the order in which they are listed.

Example.

Let $A = \{1, 2, 3\}$, $B = \{3, 1, 2\}$, and $C = \{1, 1, 2, 3, 3, 3\}$. What are the elements of A , B , and C ? How are A , B , and C related?

Is $\{0\} = 0$?

How many elements are in the set $\{1, \{1\}\}$?

For each nonnegative integer n , let $U_n = \{n, -n\}$. Find U_1 , U_2 , and U_0 .

Certain sets of numbers are so frequently referred to that they are given special names and symbols:

N or \mathbb{N} The set of all **natural numbers**

Z or \mathbb{Z} The set of all **integers**

Q or \mathbb{Q} The set of all **rational numbers**, or quotient of integers

R or \mathbb{R} The set of all **real numbers**

Note: We may additionally use superscripts to indicate further properties of these sets:

\mathbb{Z}^+ or $\mathbb{Z}^{>0}$ The set of *positive* integers

\mathbb{Q}^- or $\mathbb{Q}^{<0}$ The set of *negative* rational numbers

\mathbb{R}^{nonneg} or $\mathbb{R}^{\geq 0}$ The set of *nonnegative* real numbers

Note: Different sources denote the natural numbers \mathbb{N} as \mathbb{Z}^+ or $\mathbb{Z}^{\geq 0}$.

Definition. (Set-Builder Notation)

Let S be a set and let $P(x)$ be a property that elements of S may or may not satisfy. We may define a new set to be **the set of all elements x in S such that $P(x)$ is true**. We denote this set as follows:

$$\{x \in S \mid P(x)\}$$

↑ ↑
the set of all such that

Example. Describe each of the following sets:

$$\{x \in \mathbb{R} \mid -2 < x < 5\}$$

$$\{x \in \mathbb{Z} \mid -2 < x < 5\}$$

$$\{x \in \mathbb{Z}^+ \mid -2 < x < 5\}$$

Definition.

If A and B are sets, then A is called a **subset** of B , written $A \subseteq B$, if, and only if, every element of A is also an element of B :

$A \subseteq B$ means that for every element x , if $x \in A$, then $x \in B$.

$A \not\subseteq B$ means that there is at least one element x , such that $x \in A$ and $x \notin B$.

A is a **proper subset** of B if, and only if, every element of A is in B , but there is at least one element of B that is not in A :

$A \subsetneq B$ means that for every element x , if $x \in A$, then $x \in B$,
and there exists $x \in B$ such that $x \notin A$.

Example. Let $A = \mathbb{Z}^+$, $B = \{n \in \mathbb{Z} \mid 0 \leq n \leq 100\}$, and $C = \{100, 200, 300, 400, 500\}$. Evaluate the truth and falsity of each of the following statements.

$$B \subseteq A$$

$$C \text{ is a proper subset of } A$$

$$C \text{ and } B \text{ have at least one element in common}$$

$$C \subseteq B$$

$$C \subseteq C$$

Example. Determine which of the following statements are true:

$$2 \in \{1, 2, 3\}$$

$$\{2\} \in \{1, 2, 3\}$$

$$2 \subseteq \{1, 2, 3\}$$

$$\{2\} \subseteq \{1, 2, 3\}$$

$$\{2\} \subseteq \{\{1\}, \{2\}\}$$

$$\{2\} \in \{\{1\}, \{2\}\}$$

Definition.

Given elements a and b , the symbol (a, b) denotes the **ordered pair** consisting of a and b together with the specification that a is the first element of the pair, and b is the second element. Two ordered pairs (a, b) and (c, d) are equal if, and only if, $a = c$ and $b = d$:

$$(a, b) = (c, d) \text{ means that } a = c \text{ and } b = d.$$

Example.

Is $(1, 2) = (2, 1)$?

Is $\left(3, \frac{5}{10}\right) = \left(\sqrt{9}, \frac{1}{2}\right)$?

Definition.

Let $n \in \mathbb{N}$ and let x_1, x_2, \dots, x_n be (not necessarily distinct) elements. The **ordered n -tuple**, (x_1, x_2, \dots, x_n) , consists of x_1, x_2, \dots, x_n together with the ordering: first x_1 , then x_2 , and so forth up to x_n . An ordered 2-tuple is called an **ordered pair**, and an ordered 3-tuple is called an **ordered triple**.

Two ordered n -tuples (x_1, x_2, \dots, x_n) and (y_1, y_2, \dots, y_n) are **equal** if, and only if, $x_1 = y_1, x_2 = y_2, \dots$, and $x_n = y_n$:

$$(x_1, x_2, \dots, x_n) = (y_1, y_2, \dots, y_n) \iff x_1 = y_1, x_2 = y_2, \dots, x_n = y_n.$$

Example.

Is $(1, 2, 3, 4) = (1, 2, 4, 3)$?

Is $\left(3, (-2)^2, \frac{1}{2}\right) = \left(\sqrt{9}, 4, \frac{3}{6}\right)$?

Definition.

Given sets A_1, A_2, \dots, A_n , the **Cartesian product** of A_1, A_2, \dots, A_n , denoted

$$A_1 \times A_2 \times \cdots \times A_n$$

is the set of all ordered n -tuples (a_1, a_2, \dots, a_n) where $a_1 \in A_1, a_2 \in A_2, \dots, a_n \in A_n$:

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \dots, a_n) \mid a_1 \in A_1, a_2 \in A_2, \dots, a_n \in A_n\}$$

Example. Let $A = \{x, y\}$, $B = \{1, 2, 3\}$, and $C = \{a, b\}$. Find the following:

$$A \times B$$

$$B \times A$$

$$A \times A$$

How many elements are in $A \times B$, $B \times A$, and $A \times A$?

$$(A \times B) \times C$$

$$A \times B \times C$$

Describe $\mathbb{R} \times \mathbb{R}$

Definition.

Let $n \in \mathbb{N}$. Given a finite set A , a **string of length n over A** is an ordered n -tuple of elements of A written without parentheses or commas. The elements of A are called the **characters** of the string. The **null string** over A is defined to be the “string” with no characters, often denoted λ , and is said to have length 0. If $A = \{0, 1\}$, then a string over A is called a **bit string**.

Example. Let $A = \{a, b\}$. List all strings of length 3 over A with at least two characters that are the same.

1.3: The Language of Relations and Functions

Definition.

Let A and B be sets. A **relation R from A to B** is a subset of $A \times B$. Given an ordered pair (x, y) , x is related to y by R , written $x R y$, if, and only if, (x, y) is in R . The set A is called the **domain** of R and the set B is called its **co-domain**.

The notation for a relation R may be written symbolically as follows:

$$x R y \text{ means that } (x, y) \in R.$$

The notation $x \not R y$ means that x is not related to y by R :

$$x \not R y \text{ means that } (x, y) \notin R.$$

Example. Let $A = \{1, 2\}$ and $B = \{1, 2, 3\}$ and define a relation R from A to B as follows; Given any $(x, y) \in A \times B$,

$$(x, y) \in R \text{ means that } \frac{x - y}{2} \text{ is an integer.}$$

State explicitly which ordered pairs are in $A \times B$ and which are in R

Is $1 R 3$?

Is $2 R 3$?

Is $2 R 2$?

What are the domain and co-domain of R ?

Example. Define a relation C from \mathbb{R} to \mathbb{R} as follows: For any $(x, y) \in \mathbb{R} \times \mathbb{R}$,

$(x, y) \in C$ means that $x^2 + y^2 = 1$.

Is $(1, 0) \in C$?

Is $(0, 0) \in C$?

Is $\left(-\frac{1}{2}, \frac{\sqrt{3}}{2}\right) \in C$?

Is $-2 \in C \ 0$?

Is $0 \in C \ (-1)$?

Is $1 \in C \ 1$?

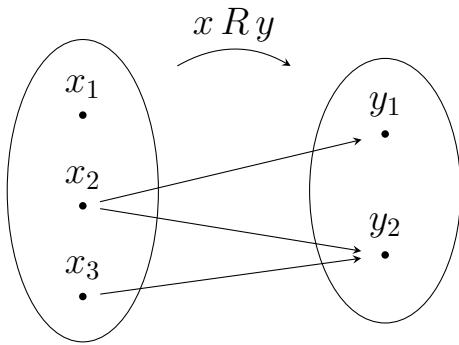
What are the domain and co-domain of C ?

Draw a graph for C by plotting the points of C in the Cartesian plane.

Definition.

Suppose R is a relation from set A to a set B . The **arrow diagram for R** is obtained as follows:

1. Represent the elements of A as points in one region and the elements of B as points in another region.
2. For each x in A and y in B , draw an arrow from x to y if, and only if, x is related to y by R .

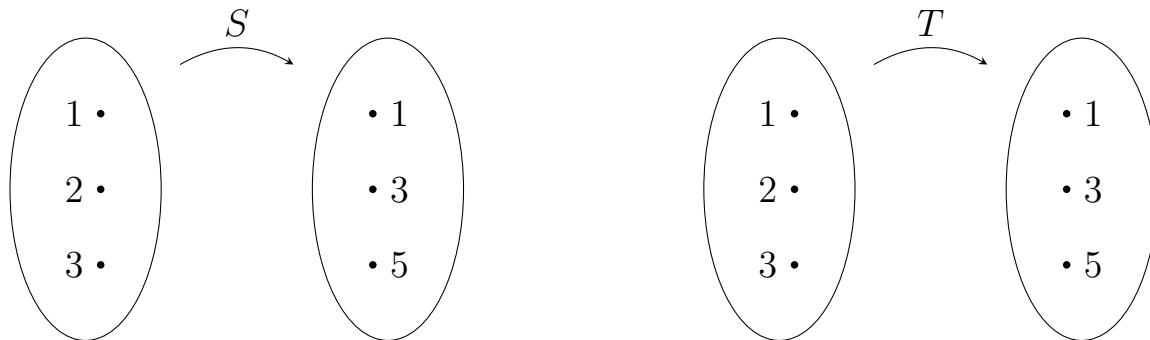


Example. Let $A = \{1, 2, 3\}$ and $B = \{1, 3, 5\}$ and define relations S and T from A to B as follows: For every $(x, y) \in A \times B$,

$(x, y) \in S$ means that $x < y$

$$T = \{(2, 1), (2, 5)\}.$$

Draw arrow diagrams for S and T



Definition.

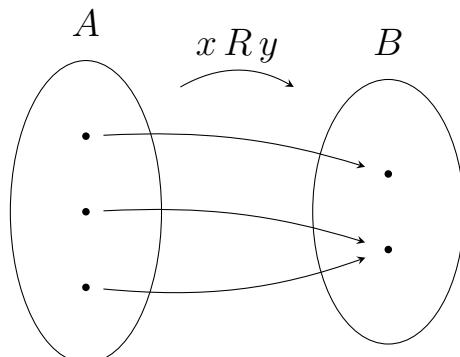
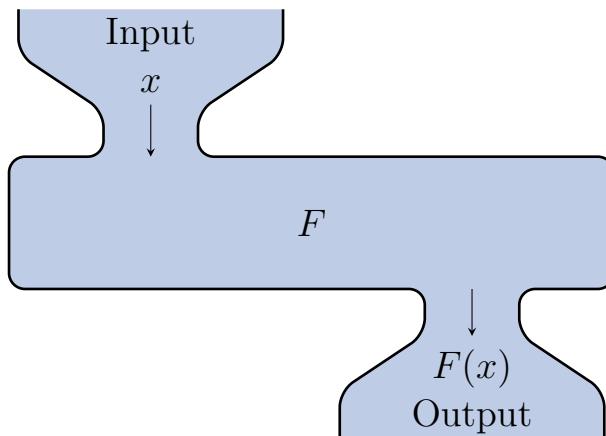
A **function F from a set A to a set B** is a relation with domain A and co-domain B that satisfies the following two properties:

1. For every element x in A , there is an element y in B such that $(x, y) \in F$.
2. For all elements x in A and y and z in B ,
if $(x, y) \in F$ and $(x, z) \in F$, then $y = z$.

Note: A relation from A to B is a function if, and only if,

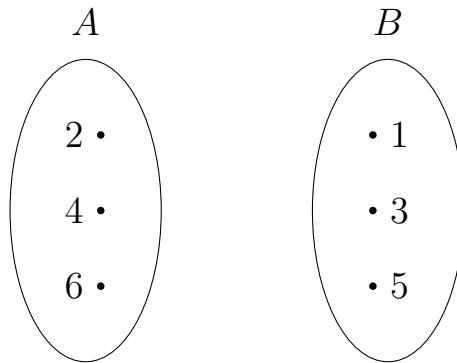
1. Every element of A is the first element of an ordered pair of F
2. No two distinct ordered pairs in F have the same first element.

Note: If A and B are sets and F is a function from A to B , then given any element x in A , the unique element in B that is related to x by F is denoted $F(x)$, which is read “ F of x ”.

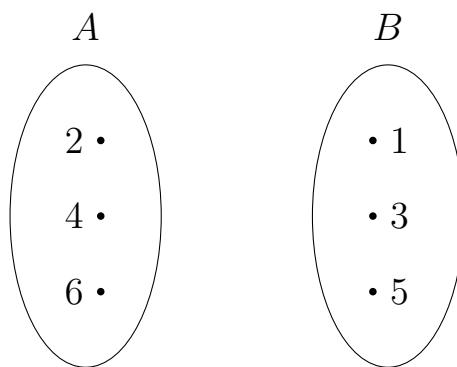


Example. Let $A = \{2, 4, 6\}$ and $B = \{1, 3, 5\}$. Which of the relations R , S , and T defined below are functions from A to B ?

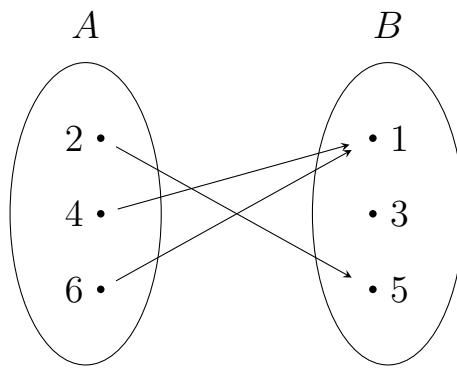
$$R = \{(2, 5), (4, 1), (4, 3), (6, 5)\}$$



For every $(x, y) \in A \times B$, $(x, y) \in S$ means that $y = x + 1$.



T is defined by the arrow diagram



2.1: Logical Form and Logical Equivalence

Definition.

A **statement** (or **proposition**) is a sentence that is true or false, but not both.

Example. Determine which of the following are statements:

$$2 + 2 = 4$$

$$2 + 2 = 5$$

$$x^2 + 2 = 11$$

Today is Saturday.

She is a computer science major.

Jane is a computer science major.

Definition. (Compound Statements)

Let p and q be statement variables.

- The **negation** of p is “not p ”, and is denoted as $\sim p$ (or $\neg p$)
- The **conjunction** of p and q is “ p and q ”, and is denoted at $p \wedge q$
- The **disjunction** of p and q is “ p or q ”, and is denoted $p \vee q$.
- The **exclusive or** of p and q is “ p x-or q ”, and is denoted $p \oplus q$ (or p XOR q)

The **order of operations** specifies that \sim is performed first.

Example. Consider the following statements:

$$\begin{aligned} p &: \text{It is raining.} \\ q &: \text{It is sunny.} \\ r &: \text{It is cloudy.} \end{aligned}$$

Rewrite the following compound statements in words:

$$\sim p$$

$$p \vee q$$

$$q \wedge r$$

$$q \wedge \sim r$$

$$p \wedge (q \vee r)$$

$$p \oplus q$$

Definition.

A **statement form** (or **propositional form**) is an expression made up of statement variables (e.g., p , q , and r), and logical connectives (e.g. \sim , \wedge , \vee , and \oplus).

The **truth table** for a given statement form displays the truth values that correspond to all possible combinations of truth values for its component statement variables.

Example. Let p and q be statement variables. Fill out the following truth tables:

| p | $\sim p$ |
|-----|----------|
| T | |
| F | |

| p | q | $p \wedge q$ | $p \vee q$ | $p \oplus q$ |
|-----|-----|--------------|------------|--------------|
| T | T | | | |
| T | F | | | |
| F | T | | | |
| F | F | | | |

| p | q | $p \vee q$ | $p \wedge q$ | $\sim(p \wedge q)$ | $(p \vee q) \wedge \sim(p \wedge q)$ |
|-----|-----|------------|--------------|--------------------|--------------------------------------|
| T | T | | | | |
| T | F | | | | |
| F | T | | | | |
| F | F | | | | |

Example. Construct a truth table for the statement form $(p \wedge q) \vee \sim r$.

Definition.

Two *statement forms* are called **logically equivalent** if, and only if, they have identical true values for each possible substitution of statements for their statement variables. The logical equivalence of statement forms P and Q is denoted $P \equiv Q$.

Example. Use truth tables to test if the following statement forms are equivalent:

$$p \text{ and } \sim(\sim p)$$

$$\sim(p \wedge q) \text{ and } \sim p \wedge \sim q$$

Definition. (De Morgan's Laws)

The negation of an *and* statement is logically equivalent to the *or* statement in which each component is negated.

The negation of an *or* statement is logically equivalent to the *and* statement in which each component is negated.

Example. Use truth tables to show that the following statement forms are equivalent:

$$\sim(p \wedge q) \text{ and } \sim p \vee \sim q$$

$$\sim(p \vee q) \text{ and } \sim p \wedge \sim q$$

Example. Using De Morgan's law to write the negation of the following statements:

Jim is at least 6 feet tall and weighs at least 200 pounds.

The bus was late or Tom's watch was slow.

$$-1 < x \leq 4$$

Definition.

A **tautology** is a statement form that is always true.

A **contradiction** is a statement form that is always false.

Example. Complete the truth tables for $p \wedge \sim p$ and $p \vee \sim p$

Example. Let **t** be a tautology, and **c** be a contradiction. Show that $p \wedge \mathbf{t} \equiv p$ and $p \wedge \mathbf{c} \equiv \mathbf{c}$

Theorem 2.1.1 Logical Equivalences (p 49)

Given any statement variables p , q , and r , a tautology \mathbf{t} and a contradiction \mathbf{c} , the following logical equivalences hold:

1. Commutative laws:

$$p \wedge q \equiv q \wedge p$$

$$p \vee q \equiv q \vee p$$

2. Associative laws:

$$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$$

$$(p \vee q) \vee r \equiv p \vee (q \vee r)$$

3. Distributive laws:

$$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$$

$$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$$

4. Identity laws:

$$p \wedge \mathbf{t} \equiv p$$

$$p \vee \mathbf{c} \equiv p$$

5. Negation laws:

$$p \vee \sim p \equiv \mathbf{t}$$

$$p \wedge \sim p \equiv \mathbf{c}$$

6. Double negative law:

$$\sim (\sim p) \equiv p$$

7. Idempotent laws:

$$p \wedge p \equiv p$$

$$p \vee p \equiv p$$

8. Universal bound laws:

$$p \vee \mathbf{t} \equiv \mathbf{t}$$

$$p \wedge \mathbf{c} \equiv \mathbf{c}$$

9. De Morgan's laws:

$$\sim (p \wedge q) \equiv \sim p \vee \sim q$$

$$\sim (p \vee q) \equiv \sim p \wedge \sim q$$

10. Absorption laws:

$$p \wedge (p \vee q) \equiv p$$

$$p \wedge (p \vee q) \equiv p$$

11. Negations of \mathbf{t} and \mathbf{c} :

$$\sim \mathbf{t} \equiv \mathbf{c}$$

$$\sim \mathbf{c} \equiv \mathbf{t}$$

2.2: Conditional Statements

Definition.

If p and q are statement variables, the **conditional** of q by p is “If p then q ”, or “ p implies q ” and is denoted by $p \rightarrow q$. It is false when p is true and q is false; otherwise it is true. We call p the **hypothesis** (or **antecedent**) of the conditional and q the **conclusion** (or **consequent**).

A conditional statement that is always true because the hypothesis is false is called **vacuously true**.

If $\underbrace{4,686 \text{ is divisible by } 6}_{\text{hypothesis}}$, then $\underbrace{4,686 \text{ is divisible by } 3}_{\text{conclusion}}$

Example. Consider the following statement:

If Lander is open, then we will have class.

Create the truth table for $p \rightarrow q$

| p | q | $p \rightarrow q$ |
|-----|-----|-------------------|
| T | T | |
| T | F | |
| F | T | |
| F | F | |

Note: The **order of operations** states that \rightarrow is performed last

Example. Create the truth table for $p \vee \sim q \rightarrow \sim p$.

| p | q | $\sim q$ | $p \vee \sim q$ | $\sim p$ | $p \vee \sim q \rightarrow \sim p$ |
|-----|-----|----------|-----------------|----------|------------------------------------|
| T | T | F | T | F | F |
| T | F | T | T | F | F |
| F | T | F | F | T | T |
| F | F | T | T | T | T |

Example. Use a truth table to show that $p \vee q \rightarrow r \equiv (p \rightarrow r) \wedge (q \rightarrow r)$

| p | q | r | $p \vee q$ | $p \vee q \rightarrow r$ | $p \rightarrow r$ | $q \rightarrow r$ | $(p \rightarrow r) \wedge (q \rightarrow r)$ |
|-----|-----|-----|------------|--------------------------|-------------------|-------------------|--|
| T | T | T | T | T | T | T | T |
| T | T | F | T | T | F | F | F |
| T | F | T | T | T | F | T | F |
| T | F | F | T | T | F | F | F |
| F | T | T | T | T | T | T | T |
| F | T | F | T | T | F | F | F |
| F | F | T | F | F | T | T | T |
| F | F | F | F | F | T | F | F |

Definition.

The **negation** of “if p then q ” is logically equivalent to “ p and not q ”:

$$\sim(p \rightarrow q) \equiv p \wedge \sim q$$

Example. Write negations for each of the following statements:

If my car is in the repair shop, then I cannot get to class.

If Sara lives in Athens, then she lives in Greece.

Definition.

The **contrapositive** of a conditional statement of the form “If p then q ” is

$$\text{If } \sim q \text{ then } \sim p : \sim q \rightarrow \sim p$$

A conditional statement is logically equivalent to its contrapositive.

Example. Write each of the following statements in its equivalent contrapositive form:

If Howard can swim across the lake, then Howard can swim to the island.

If today is Easter, then tomorrow is Monday.

Definition.

Suppose a conditional statement of the form “If p then q ” is given.

- The **converse** is “If q then p ”: $q \rightarrow p$
- The **inverse** is “If $\sim p$ then $\sim q$ ”: $\sim p \rightarrow \sim q$

Example. Write the converse and inverse of each of the following statements:

If Howard can swim across the lake, then Howard can swim to the island.

Converse:

Inverse:

If today is Easter, then tomorrow is Monday.

Converse:

Inverse:

Note:

1. A conditional statement and its converse are *not* logically equivalent.
2. A conditional statement and its inverse are *not* logically equivalent.
3. The converse and the inverse of a conditional statement are logically equivalent to each other.

Definition.

If p and q are statements, p **only if** q means “if not q then not p ”:

$$\sim q \rightarrow \sim p \equiv p \rightarrow q$$

Example. Rewrite the following statement in if-then form in two ways, one of which is the contrapositive of the other:

John will break the world’s record for the mile run only if he runs the mile in under four minutes.

$$\sim q \rightarrow \sim p$$

$$p \rightarrow q$$

Note:

1. “ p only if q ” does *not* mean p if q
2. It is possible for “ p only if q ” to be true at the same time that “ p if q ” is false.

e.g.: If John runs a mile in under four minutes, he still might not be fast enough to break the record.

Definition.

Given statement variables p and q , the **biconditional of p and q** is “ p if, and only if, q ” and is denoted $p \leftrightarrow q$. It is true if both p and q have the same truth values and is false otherwise. The words *if and only if* are sometimes abbreviated **iff**.

Note: The **order of operations** states that \leftrightarrow is coequal with \rightarrow

Example. Create the truth table for $p \leftrightarrow q$

| p | q | $p \leftrightarrow q$ |
|-----|-----|-----------------------|
| T | T | |
| T | F | |
| F | T | |
| F | F | |

Order of Operations for Logical Operators

- \sim Evaluate negations first
- \wedge, \vee Evaluate \wedge and \vee second. When both present, parentheses may be needed.
- $\rightarrow, \leftrightarrow$ Evaluate \rightarrow and \leftrightarrow third. When both present, parentheses may be needed.

Definition.

If r and s are statements:

1. r is a **sufficient condition** for s means “if r then s ”. $r \rightarrow s$
2. r is a **necessary condition** for s means “if not r then not s ”. $\sim r \rightarrow \sim s$

By property of the contrapositive:

3. r is a *necessary and sufficient condition* for s means “ r if, and only if s . $r \leftrightarrow s$

Example. Rewrite the following statement in the form “If A then B ”:

Having two 45° angles is a sufficient condition for this triangle to be a right triangle.

Example. Use the contrapositive to rewrite the following statement in two ways:

George’s attaining age 35 is a necessary condition for his being president of the United States.

2.5: Application: Number Systems and Circuits for Addition

Recall our how we write numbers in base 10:

$$\begin{aligned}5,049 &= 5 \cdot 1000 + 0 \cdot 100 + 4 \cdot 10 + 9 \cdot 1 \\&= 5 \cdot 10^3 + 0 \cdot 10^2 + 4 \cdot 10^1 + 9 \cdot 10^0\end{aligned}$$

Definition.

Any integer $b > 1$ can be used as a base for a numbering system. A numbering system of base b has the digits $0, 1, \dots, b - 1$.

A **base 2 notation** or **binary notation**, uses the digits 0, 1. In binary, every integer is represented as sum of products of the form

$$d \cdot 2^n$$

where $n \in \mathbb{Z}$ and $d \in \{0, 1\}$.

Example. Below is the binary representation for the integers 1 to 9:

$$\begin{array}{lllll}1_{10} & = & 1 \cdot 2^0 & = & 1_2 \\2_{10} & = & 1 \cdot 2^1 + 0 \cdot 2^0 & = & 10_2 \\3_{10} & = & 1 \cdot 2^1 + 1 \cdot 2^0 & = & 11_2 \\4_{10} & = & 1 \cdot 2^2 + 0 \cdot 2^1 + 0 \cdot 2^0 & = & 100_2 \\5_{10} & = & 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 & = & 101_2 \\6_{10} & = & 1 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0 & = & 110_2 \\7_{10} & = & 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 & = & 111_2 \\8_{10} & = & 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 0 \cdot 2^0 & = & 1000_2 \\9_{10} & = & 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 & = & 1001_2\end{array}$$

Converting binary → decimal:

To convert from binary to decimal, multiply each digit by its corresponding power of 2 and sum the results.

Example. Represent the following in decimal notation (base-10):

$$110_2$$

$$1011_2$$

$$11110_2$$

$$101011_2$$

Converting decimal → binary:

To convert from decimal to binary, we repeated divide by 2, and record the remainders.

Example.

$$\begin{aligned}27_{10} &= 16 + 8 + 2 + 1 \\&= 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 \\&= 11011_2\end{aligned}$$

Example. Represent the following in binary notation:

$$243_{10}$$

$$587_{10}$$

$$990_{10}$$

$$531_{10}$$

Binary arithmetic:

In binary arithmetic, 10_2 behaves similarly to 10 in decimal arithmetic.

Example. Add 1101_2 and 111_2 using binary notation.

Example. Subtract 1011_2 from 11000_2 using binary notation.

Definition.

The **8-bit two's complement** for an integer a between -128 and 127 is the 8-bit binary representation for

$$\begin{cases} a, & \text{if } a \geq 0 \\ 2^8 - |a|, & \text{if } a < 0. \end{cases}$$

Two's complement allows maximum representation for 2^8 integers with 8 binary digits.

Example. Below are a few integers represented in binary using 8-bit two's complement:

$$-128 \rightarrow 2^8 - |-128| = 128_{10} = 10000000_2 \quad 0 \rightarrow 0_{10} = 00000000_2$$

$$-127 \rightarrow 2^8 - |-127| = 129_{10} = 10000001_2 \quad 1 \rightarrow 1_{10} = 00000001_2$$

$$\vdots \quad 2 \rightarrow 2_{10} = 00000010_2$$

$$-2 \rightarrow 2^8 - |-2| = 254_{10} = 10000000_2 \quad \vdots$$

$$-1 \rightarrow 2^8 - |-1| = 255_{10} = 11111111_2 \quad 127 \rightarrow 127_{10} = 01111111_2$$

Example. Find the 8-bit two's complement for the following:

-46

42

120

-82

Two's complement of a negative integer:

To find the decimal representation of the negative integer with a given 8-bit two's complement:

- Flip the bits
- Add 1
- Convert to base-10 and swap the sign

Example. Find the decimal representation of the integers with the following 8-bit two's complement:

11100101_2

11000000_2

Addition and Subtraction with Integers in Two's Complement Form:

When performing binary addition on integers written in Two's Complement form, we discard any “carry” bit.

Example. Perform binary addition using the Two's Complement form of the following:

83 and -55

-87 and -46

Definition.

Hexadecimal notation uses a **base 16 notation**. In hexadecimal, every integer is represented as sum of products of the form

$$d \cdot 16^n$$

where $n \in \mathbb{Z}$ and $d \in \{0, 1, \dots, 9, A, B, C, D, E, F\}$.

| Decimal | Hexadecimal | 4-Bit Binary |
|---------|-------------|--------------|
| 0 | 0 | 0000 |
| 1 | 1 | 0001 |
| 2 | 2 | 0010 |
| 3 | 3 | 0011 |
| 4 | 4 | 0100 |
| 5 | 5 | 0101 |
| 6 | 6 | 0110 |
| 7 | 7 | 0111 |
| 8 | 8 | 1000 |
| 9 | 9 | 1001 |
| 10 | A | 1010 |
| 11 | B | 1011 |
| 12 | C | 1100 |
| 13 | D | 1101 |
| 14 | E | 1110 |
| 15 | F | 1111 |

Example. Convert $3CF_{16}$ to decimal notation.

Example. Convert $B09F_{16}$ to binary notation.

Example. Convert 100110110101001_2 to hexadecimal notation.

3.1: Predicates and Quantified Statements I

Definition.

A **predicate** is a sentence that contains a finite number of variables and becomes a statement when specific values are substituted for the variables.

The **domain** of a predicate variable is the set of all values that may be substituted in place of the variable.

Example. Let $P(x)$ be the predicate “ $x^2 > x$ ” with domain the set \mathbb{R} . Write $P(2)$, $P\left(\frac{1}{2}\right)$, and $P\left(-\frac{1}{2}\right)$, and indicate which of these statements are true and which are false.

Definition.

If $P(x)$ is a predicate and x has domain D , the **truth set** of $P(x)$ is the set of all elements of D that make $P(x)$ true when they are substituted for x . The truth set of $P(x)$ is denoted

$$\{x \in D \mid P(x)\}$$

Example. Let $Q(n)$ be the predicate “ n is a factor of 8”. Find the truth set of $Q(n)$ if

the domain of n is \mathbb{Z}^+

the domain of n is \mathbb{Z}

Definition.

Let $Q(x)$ be a predicate and D the domain of x .

- **Quantifiers** are words that refer to quantities such as “some” or “all” and tell for how many elements a given predicate is true.
- The **universal quantifier** is represented by the symbol “ \forall ”.
- A **universal statement** is a statement of the form “ $\forall x \in D, Q(x)$ ”.
 - It is defined to be true if, and only if, $Q(x)$ is true for *each* individual x in D .
 - It is defined to be false if, and only if, $Q(x)$ is false for *at least one* x in D .
- A value for x for which $Q(x)$ is false is called a **counterexample** to the universal statement.

Example. Let $D = \{1, 2, 3, 4, 5\}$, and consider the statement

$$\forall x \in D, x^2 \geq x.$$

Write one way to read this statement out loud, and show that it is true.

The above example uses the **method of exhaustion**.

Example. Consider the statement

$$\forall x \in \mathbb{R}, x^2 \geq x.$$

Find a counter example to show that this statement is false.

Definition.

Let $Q(x)$ be a predicate and D the domain of x .

- The **existential quantifier** is represented by the symbol “ \exists ”.
- An **existential statement** is a statement of the form “ $\exists x \in D$ such that $Q(x)$ ”.
 - It is defined to be true if, and only if, $Q(x)$ is true for *at least one* x in D .
 - It is false if, and only if, $Q(x)$ is false *for all* x in D .

Example. Consider the statement

$$\exists m \in \mathbb{Z}^+ \text{ such that } m^2 = m.$$

Write one way to read this statement out loud, and show that it is true.

Example. Let $E = \{5, 6, 7, 8\}$ and consider the statement

$$\exists m \in E \text{ such that } m^2 = m.$$

Show that this statement is false.

Example. Rewrite the following statements formally using quantifiers and variables:

All triangles have three sides.

No dogs have wings.

Some programs are structured.

Definition.

A **universal conditional statement** is of the form:

$$\forall x, \text{ if } P(x) \text{ then } Q(x).$$

Example. Rewrite each of the following statements in the form

$$\forall \underline{\quad}, \text{ if } \underline{\quad} \text{ then } \underline{\quad}$$

If a real number is an integer, then it is a rational number.

All bytes have eight bits.

No fire trucks are green.

3.2: Predicates and Quantified Statements II

Definition.

- The negation of a statement of the form

$$\forall x \text{ in } D, Q(x)$$

is logically equivalent to a statement of the form

$$\exists x \text{ in } D \text{ such that } \sim Q(x).$$

$$\sim (\forall x \in D, Q(x)) \equiv \exists x \in D \text{ such that } \sim Q(x).$$

- The negation of a statement of the form

$$\exists x \text{ in } D \text{ such that } Q(x)$$

is logically equivalent to a statement of the form

$$\forall x \text{ in } D, \sim Q(x).$$

$$\sim (\exists x \in D \text{ such that } Q(x)) \equiv \forall x \in D, \sim Q(x)$$

Example. Negate the following statements:

$$\forall \text{ primes } p, p \text{ is odd}$$

$$\exists \text{ a triangle } T \text{ such that the sum of the angles of } T \text{ equals } 200^\circ$$

Example. Rewrite the following statements formally, then write the formal and informal negations.

No politicians are honest

The number 1,357 is not divisible by any integer between 1 and 37.

Example. Write informal negations for the following statements:

All computer programs are finite.

Some computer hackers are over 40.

Negation of a Universal Conditional Statement

$$\sim (\forall x, \text{ if } P(x) \text{ then } Q(x)) \equiv \exists x \text{ such that } P(x) \text{ and } \sim Q(x)$$

Definition.

A statement of the form

$$\forall x \text{ in } D, \text{ if } P(x) \text{ then } Q(x)$$

is called **vacuously true** or **true by default** if, and only if, $P(x)$ is false for every x in D .

Example. The following statement is vacuously true since it's negation is false:

All kangaroos enrolled in my class are passing.

Definition.

Consider a statement of the form $\forall x \in D$, if $P(x)$ then $Q(x)$.

1. Its **contrapositive** is the statement $\forall x \in D$, if $\sim Q(x)$ then $\sim P(x)$.
2. Its **converse** is the statement $\forall x \in D$, if $Q(x)$ then $P(x)$.
3. Its **inverse** is the statement $\forall x \in D$, if $\sim P(x)$ then $\sim Q(x)$.

Example. Write a formal and informal contrapositive, converse, and inverse for the following statement:

If a real number is greater than 2, then its square is greater than 4.

Definition.

- “ $\forall x, r(x)$ is a **sufficient condition** for $s(x)$ ” \rightarrow “ $\forall x, \text{if } r(x) \text{ then } s(x)$ ”
- “ $\forall x, r(x)$ is a **necessary condition** for $s(x)$ ” \rightarrow “ $\forall x, \text{if } \sim r(x) \text{ then } \sim s(x)$ ”
 \rightarrow “ $\forall x, \text{if } s(x) \text{ then } r(x)$ ”
- “ $\forall x, r(x)$ **only if** $s(x)$ ” \rightarrow “ $\forall x, \text{if } \sim s(x), \text{ then } \sim r(x)$ ”
 \rightarrow “ $\forall x, \text{if } r(x) \text{ then } s(x)$ ”

Example. Rewrite each of the following as a universal conditional statement, quantified either explicitly or implicitly. Do not use the word *necessary* or *sufficient*.

Squareness is a sufficient condition for rectangularity.

Being at least 35 years old is a necessary condition for being president of the United States.

Example. Rewrite the following as a universal conditional statement:

A product of two numbers is 0 only if one of the numbers is 0.

6.1: Set Theory: Definitions and the Element Method of Proof

Element Argument: The Basic Method for Proving that One set is a Subset of Another

Let sets X and Y be given. To prove that $X \subseteq Y$,

1. suppose that x is a particular but arbitrarily chosen element of X ,
2. show that x is an element of Y

Example. Define sets A and B as follows:

$$A = \{m \in \mathbb{Z} \mid m = 6r + 12 \text{ for some } r \in \mathbb{Z}\}$$

$$B = \{n \in \mathbb{Z} \mid n = 3s \text{ for some } s \in \mathbb{Z}\}$$

Prove that $A \subseteq B$

Disprove that $B \subseteq A$

Definition.

Given sets A and B , A **equals** B , written $\mathbf{A} = \mathbf{B}$, if, and only if, every element of A is in B and every element of B is in A :

$$A = B \Leftrightarrow A \subseteq B \text{ and } B \subseteq A.$$

Example. Define sets A and B as follows:

$$A = \{m \in \mathbb{Z} \mid m = 6r + 12 \text{ for some } r \in \mathbb{Z}\}$$

$$B = \{n \in \mathbb{Z} \mid n = 3s \text{ for some } s \in \mathbb{Z}\}$$

Is $A = B$?

Definition.

Given an integer n and a positive integer d , when n is divided by d , then

$$n \text{ div } d = \text{ the integer quotient}$$
$$n \text{ mod } d = \text{ the nonnegative integer remainder}$$

If n and d are integers and $d > 0$, then

$$n \text{ div } d = q \quad \text{and} \quad n \text{ mod } d = r \quad \Leftrightarrow \quad n = dq + r$$

Example. Compute the following:

$$32 \text{ div } 9, \quad 32 \text{ mod } 9$$

$$365 \text{ div } 7, \quad 365 \text{ mod } 7$$

Example. If it is currently 11:00, what time will it be in

$$51 \text{ hours?}$$

$$121 \text{ hours?}$$

$$11 \text{ hours?}$$

$$-1 \text{ hours?}$$

Example. Let $A = \{4, \sqrt{16}, 19 \text{ mod } 15\}$ and $B = \{12 \text{ mod } 8\}$. Is $A \subseteq B$? Is $B \subseteq A$?

Definition.

Let A and B be subsets of a universal set U .

1. The **union** of A and B is the set of all elements that are in at least one of A or B .

$$A \cup B = \{x \in U \mid x \in A \text{ or } x \in B\}$$

2. The **intersection** of A and B is the set of all elements that are common to both A and B .

$$A \cap B = \{x \in U \mid x \in A \text{ and } x \in B\}$$

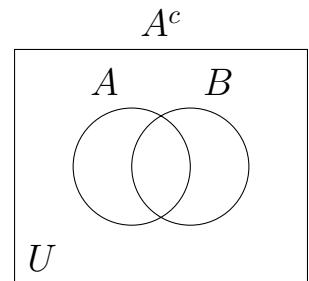
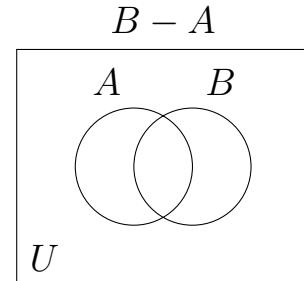
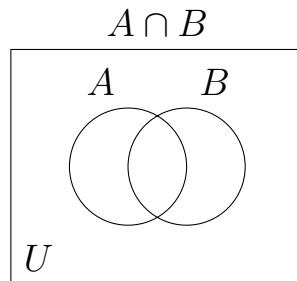
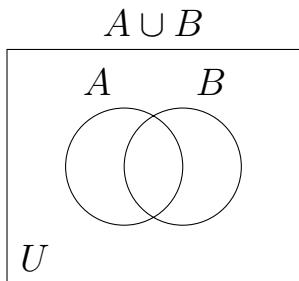
3. The **difference** of A and B is the set of all elements that are in B and not A .

$$B - A = \{x \in U \mid x \in B \text{ and } x \notin A\}$$

4. The **complement** of A is the set of all elements in U that are not in A .

$$A^c = \{x \in U \mid x \notin A\}$$

Example. Represent the following sets using the Venn diagrams below:



Example. Let the universal set be the set $U = \{a, b, c, d, e, f, g\}$, and let $A = \{a, c, e, g\}$ and $B = \{d, e, f, g\}$. Find

$$A \cup B$$

$$A \cap B$$

$$B - A$$

$$A^c$$

Definition.

Given real numbers a and b with $a \leq b$:

$$(a, b) = \{x \in \mathbb{R} \mid a < x < b\}$$

$$[a, b) = \{x \in \mathbb{R} \mid a \leq x < b\}$$

$$(a, b] = \{x \in \mathbb{R} \mid a < x \leq b\}$$

$$[a, b] = \{x \in \mathbb{R} \mid a \leq x \leq b\}$$

Example. Let the universal set be \mathbb{R} , and let $A = (-1, 0]$ and $B = [0, 1)$. Find

$$A \cup B$$

$$A \cap B$$

$$B - A$$

$$A^c$$

Definition.

Given sets A_0, A_1, A_2, \dots that are subsets of a universal set U and given a nonnegative integer n ,

$$\bigcup_{i=0}^n A_i = \{x \in U \mid x \in A_i, \text{ for at least one } i = 0, 1, 2, \dots, n\}$$

$$\bigcap_{i=0}^n A_i = \{x \in U \mid x \in A_i, \text{ for every } i = 0, 1, 2, \dots, n\}$$

Example. For each positive integer i , let $A_i = \left\{x \in \mathbb{R} \mid -\frac{1}{i} < x < \frac{1}{i}\right\} = \left(-\frac{1}{i}, \frac{1}{i}\right)$.
Find

$$A_1 \cup A_2 \cup A_3$$

$$A_1 \cap A_2 \cap A_3$$

$$\bigcup_{i=1}^{\infty} A_i$$

$$\bigcap_{i=1}^{\infty} A_i$$

Definition.

The **empty set** (or **null set**), denoted \emptyset , is the set with no elements.

$$\{1, 3\} \cap \{2, 4\} = \emptyset$$

Two sets are called **disjoint** if, and only if, they have no elements in common:

$$A \cap B = \emptyset.$$

Sets A_1, A_2, A_3, \dots are **mutually disjoint** (or **pairwise disjoint**) if, and only if, no two sets A_i and A_j with distinct subscripts have any elements in common:

$$A_i \cap A_j = \emptyset \text{ whenever } i \neq j.$$

Example.

Let $A_1 = \{3, 5\}$, $A_2 = \{1, 4, 6\}$, and $A_3 = \{2\}$. Are A_1 , A_2 , and A_3 mutually disjoint?

Let $B_1 = \{2, 4, 6\}$, $B_2 = \{3, 7\}$, and $B_3 = \{4, 5\}$. Are B_1 , B_2 , B_3 mutually disjoint?

Definition.

A finite or infinite collection of nonempty sets $\{A_1, A_2, A_3, \dots\}$ is a **partition** of a set A if, and only if,

1. A is the union of all the A_i ;
2. the sets A_1, A_2, A_3, \dots are mutually disjoint.

Example.

Let $A = \{1, 2, 3, 4, 5, 6\}$, $A_1 = \{1, 2\}$, $A_2 = \{3, 4\}$, and $A_3 = \{5, 6\}$. Is $\{A_1, A_2, A_3\}$ a partition of A ?

Let \mathbb{Z} be the set of all integers and let

$$T_i = \{n \in \mathbb{Z} \mid n = 3k + i, \text{ for some integer } k\}.$$

Is $\{T_0, T_1, T_2\}$ a partition of \mathbb{Z} ?

Definition.

Given a set A , the **power set** of A , denoted $\mathcal{P}(A)$, is the set of all subsets of A .

Example. Find $\mathcal{P}(\{x, y\})$.

6.4: Boolean Algebras, Russell's Paradox, and the Halting Problem

Definition.

A **Boolean algebra** is a set B together with two operations, generally denoted $+$ and \cdot , such that for all a and b in B both $a + b$ and $a \cdot b$ are in B and the following axioms are assumed to hold:

1. *Commutative Laws:* For all a and b in B ,

$$a + b = b + a \text{ and } a \cdot b = b \cdot a$$

2. *Associative Laws:* For all a and b in B ,

$$(a + b) + c = a + (b + c) \text{ and } (a \cdot b) \cdot c = a \cdot (b \cdot c)$$

3. *Distributive Laws:* For all a and b in B ,

$$a + (b \cdot c) = (a + b) \cdot (a + c) \text{ and } a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

4. *Identity Laws:* There exist distinct elements 0 and 1 in B such that for each a in B ,

$$a + 0 = a \text{ and } a \cdot 1 = a$$

5. *Complement Laws:* For each a in B , there exists an element in B , denoted \bar{a} and called the **complement** or **negation** of a , such that

$$a + \bar{a} = 1 \text{ and } a \cdot \bar{a} = 0$$

Properties of a Boolean Algebra

Let B be any Boolean algebra.

1. *Uniqueness of the Complement Laws:* For all a and x in B , if $a + x = 1$ and $a \cdot x = 0$, then $x = \bar{a}$.
2. *Uniqueness of 0 and 1:* If there exists x in B such that $a + x = a$ for every a in B , then $x = 0$, and if there exists y in B such that $a \cdot y = a$ for every a in B , then $y = 1$.
3. *Double Complement Law:* For every $a \in B$, $\overline{\overline{a}} = a$.
4. *Idempotent Laws:* For every $a \in B$,

$$a + a = a \text{ and } a \cdot a = a.$$

5. *Universal Bound Laws:* For every $a \in B$,

$$a + 1 = 1 \text{ and } a \cdot 0 = 0.$$

6. *De Morgan's Laws:* For all a and $b \in B$,

$$\overline{a + b} = \bar{a} \cdot \bar{b} \text{ and } \overline{a \cdot b} = \bar{a} + \bar{b}.$$

7. *Absorption Laws:* For all a and $b \in B$,

$$(a + b) \cdot a = a \text{ and } (a \cdot b) + a = a.$$

8. *Complements of 0 and 1:*

$$\overline{0} = 1 \text{ and } \overline{1} = 0.$$

Example. Prove that for all elements a in a Boolean algebra B :

$$\overline{(\bar{a})} = a.$$

$$a + a = a.$$

Example. Prove that for all elements a in a Boolean algebra B :

$$a \cdot a = a.$$

$$(a + b) \cdot a = a.$$

Russell's Paradox

Define the following set S :

$$S = \{A \mid A \text{ is a set and } A \notin A\}.$$

Is S an element of itself?

The Barber Puzzle: In a certain town, there is a male barber who shaves all those men, and only those men, who do not shave themselves.

Does the barber shave himself?

Is the sentence “The barber shaves himself” a statement?

Example. Determine whether each sentence is a statement:

If $1 + 1 = 3$, then $1 = 0$.

This sentence is false and $1 + 1 = 3$.

The Halting Problem (Alan M. Turing)

There is no computer algorithm that will accept any algorithm X and data set D as input and then will output “halts” or “loops forever” to indicate whether or not X terminates in a finite number of steps when X is run with data set D .